

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS

No. 4:25-cv-00209

Strike 3 Holdings, LLC,
Plaintiff,

v.

John Doe,
Defendant.

OPINION AND ORDER

Before the court is plaintiff's motion for leave to serve a third-party subpoena on an internet-service provider, Frontier Communications Corporation, in order to obtain the name and address of the unidentified defendant. Doc. 5. For the reasons set forth below, that motion is granted in part.

Plaintiff is an adult-films owner whose works the John Doe defendant is allegedly copying on a large scale in violation of plaintiff's ownership rights in the material. Doc. 1. Using a torrent collector, plaintiff has purportedly identified defendant's IP address. Plaintiff now seeks to compel the internet-service provider (ISP) to turn over defendant's name and address so that defendant may be served with process. But to subpoena the ISP, plaintiff must obtain leave to engage in discovery before the parties' Rule 26 conference. *See* Fed. R. Civ. P. 26(d)(1).

For good cause, the court can grant plaintiff leave to serve a third-party subpoena in advance of the Rule 26(f) conference. *See Cothran v. Koomson*, No. 4:20-cv-00481, 2020 WL 6450498, at *1 (E.D. Tex. Nov. 3, 2020) ("Although the Federal Rules do not provide an exact standard for a court's granting such authorization, several other federal courts within the Fifth Circuit, including the Eastern District of Texas, have used a 'good cause' standard to determine whether a party is entitled to early discovery."); Fed. R. Civ. P. 26(d). In assessing whether a plaintiff has carried its burden of establishing that good cause exists, "a court must

examine the discovery request on the entirety of the record to date and the reasonableness of the request in light of all the surrounding circumstances.” *Huawei Techs. Co. v. Yiren Huang*, No. 4:17-cv-00893, 2018 WL 10127086, at *1 (E.D. Tex. Feb. 13, 2018) (quotation marks omitted). District courts have “broad discretion to tailor discovery narrowly and to dictate the sequence of discovery.” *Hunter Killer Prods., Inc. v. Boylan*, No. 3:20-cv-00306, 2021 WL 2878558, at *2 (W.D. Tex. Jan. 28, 2021) (quoting *Crawford-El v. Britton*, 523 U.S. 574, 598 (1998)).

Highly relevant to that reasonableness analysis is whether the requested information will actually identify the alleged infringer rather than an innocent third party. It is true that “there is no constitutional right . . . to anonymously engage in copyright infringement.” *Strike 3 Holdings, LLC v. Doe*, No. 4:21-cv-03319, 2021 WL 5359608, at *2 (S.D. Tex. Nov. 17, 2021). However, at the same time, individuals have a strong “interest in freedom from unjustified litigation.” *Doe v. State*, 2 F.3d 1412, 1419 n.15 (5th Cir. 1993). All of the non-infringing internet users subscribed to the ISP thus have a strong interest in not being named in a copyright-infringement lawsuit—especially one where the risk of embarrassment is so great. See *Digital Sins, Inc. v. John Does 1-245*, No. 1:11-cv-08170, 2012 WL 1744838, at *3 (S.D.N.Y. May 15, 2012) (discussing in a similar case the “potential for embarrassing the defendants, who face the possibility that plaintiff’s thus-far-unsubstantiated and perhaps erroneous allegation will be made public”).

There are at least two ways in which risk of such an error presents itself in this case. First, as discussed briefly at the hearing on this motion, the fact that a video was downloaded or distributed by a device associated with an IP address does not mean that the subscriber to the IP address is the one who downloaded or distributed the video. “Indeed, the true infringer could just as easily be a third party who had access to the internet connection, such as a son or daughter, houseguest, neighbor, or customer of a business offering an internet connection.” *Patrick Collins, Inc. v. Does*

1-4, No. 1:12-cv-02962, 2012 WL 2130557, at *1 (S.D.N.Y. June 12, 2012).

Second, it is at least conceivable that the ISP does not have a sufficiently reliable record of who was subscribed to which IP address at a particular time. Without evidence of the ISP's custodial policies, the court can only speculate about the likelihood and the ways in which the wrong subscriber could be named. Perhaps the ISP's records simply indicate who is currently subscribed to a particular IP address, and in response to a subpoena the ISP would produce the current subscriber's name and address rather than the previous, relevant subscriber. Or maybe an IP address can have multiple subscribers at a given time, and the ISP would produce personal information of all of them. Or perhaps not. However, given the gravity of the harm to be suffered by the wrongly sued internet user, these possibilities are at least likely enough to warrant a careful approach to authorizing the kind of subpoena that plaintiff wants to serve.

On the other hand, plaintiff and the public have a strong interest in the enforcement and vindication of plaintiff's copyrights. *See Bianco v. Globus Med., Inc.*, No. 2:12-cv-00147, 2014 WL 1049067, at *10 (E.D. Tex. Mar. 17, 2014) ("There is a strong public interest in vindicating the rights of owners of intellectual property."). Plaintiff has an interest in being compensated for its damages and in deterring pervasive, unauthorized dissemination of its content. The only way that plaintiff can vindicate those interests in this case is by identifying the defendant. That, in turn, requires subpoenaing the subscriber's identity from the ISP.

To balance these competing interests, courts will often authorize the subpoena, but in so doing they will often issue a protective order. *See, e.g., Hard Drive Prods., Inc. v. Does 1-59*, No. 4:12-cv-00699, 2012 WL 1096117, at *2-3 (S.D. Tex. Mar. 30, 2012). The purpose of the protective order is to allow the defendant, once identified, the opportunity to challenge the subpoena anonymously before his information is made public. This protects the individual's interest in being free from unjustified litigation

because, in the event that the wrong person is named as a defendant, that person will have the chance to make that argument before the litigation advances. A protective order of this type mitigates any harm from both types of risk mentioned above: the risk that someone other than the subscriber downloaded or distributed the content, and the risk that the ISP will produce the information of someone other than the relevant IP-address subscriber.

However, the second of those two risks can be further reduced before allowing plaintiff to subpoena the subscriber's information. Unlike the court, the ISP does have information about its recordkeeping practices and the extent to which it will be able to produce accurate information about the relevant subscriber to the IP address. It would pose virtually no additional burden on plaintiff to require it to first seek that general, recordkeeping information before seeking the invasive, personal information, and doing so has the potential to significantly reduce the risk that the ISP turns over the wrong person's information. Any risk that the ISP loses the information during the delay can be mitigated by a court order to make reasonable efforts to preserve the information.

The court therefore finds it appropriate to require plaintiff first to obtain information from the ISP pertaining to its recordkeeping. Specifically, it would be helpful in evaluating plaintiff's motion for the court to hear, from the ISP, how likely it is that the identifying information produced in response to a subpoena would actually identify the subscriber to the IP address through which the copyrighted material was downloaded or distributed. The response should describe the process by which such records are made and retrieved, but it should not include any personal information. In the event that the ISP reliably indicates that the risk of error is low enough, the court will be inclined to grant plaintiff's re-submitted motion for leave to serve a third-party subpoena.

Accordingly, plaintiff's motion (Doc. 5) is granted in part such that plaintiff may serve on the ISP a subpoena seeking general, recordkeeping information, and the motion (Doc. 5) is denied


without prejudice insofar as it seeks personal, identifying information. Plaintiff shall provide the ISP with a copy of this order upon serving the subpoena. The ISP is ordered to make reasonable efforts to preserve the records associated with the unnamed defendant's IP address, 47.186.116.203.

To protect non-infringing individuals' interests in privacy and anonymity, the court enters the following protective order.

Protective order

It is ordered that, in the event that Frontier Communications Corporation inadvertently produces personal, identifying information in response to plaintiff's subpoena served pursuant to this order, such identifying information shall be for plaintiff's attorney's eyes only and shall be kept confidential until further order of this court.

So ordered by the court on June 17, 2025.



J. CAMPBELL BARKER
United States District Judge